U.S. Department of Commerce

Office of Digital Engagement

Policy on the Approval and Use of

Social Media and Web 2.0 (SM/W2.0)

TABLE OF CONTENTS

Why This Policy Is Necessary 2

SM/W2.0 Technologies: 2

Purpose and Goals: 2

General Guidelines for the Use of SM/W2.0 Technologies in an Official Capacity: 3

(1) Department Employees: 3

(2) Guidelines for Use of SM for Operating Units: 5

(3) Hatch Act in the Workplace: 8

Applying for Official SM/W2.0 Accounts 8

General Guidelines for the Use of SM/W2.0 Technologies in an Unofficial Capacity: 8

(1) Personal and Professional Communication: 9

(2) Employee Title Use: 10

(3) Hatch Act on Personal Accounts: 11

Other Applicable Commerce Policies 11

Responsibilities of Chief Information Officers 12

Risk Assessment and Authorization for Use: 12

Terms of Service and Privacy: 12

Specific IT Security Guidelines for Using SM/W2.0 Technologies 13

Resources for Additional Information 14

WHY THIS POLICY IS NECESSARY

The Department of Commerce is committed to operating all its communications and transactions with individuals and organizations in an open and transparent way. Social media and Web 2.0 (SM/W2.0) services are an increasingly important avenue for stakeholders and members of the public to interact with the Department in an efficient, effective, and transparent manner.

SM/W2.0 TECHNOLOGIES:

SM/W2.0 services encompass many technologies, including XML feeds, wikis, blogs, social networking sites, discussion forums, collaborative research Web sites, comment features on news and video Web sites, and other mechanisms. Social media services allow the user to interact directly with the Web site or other users. The result is that Web users are able to communicate simultaneously, directly, and instantaneously with all other users on the Web site. Commonly used social media services include YouTube®, Flickr®, Facebook®, Twitter®, and Instagram®.

SM/W2.0 technologies also present new and unprecedented challenges to the security of the information technology (IT) networks and systems that Commerce and its operating units use, as well as complicate the protection of personally identifiable information (PII). Commerce's and other Federal agencies' information systems are targeted by persistent, pervasive, and aggressive threats. These threats may be directed against the network infrastructure or IT systems, as well as records or information in the systems, especially PII or other sensitive information. The rapid development of Web 2.0 technologies and their emerging capabilities and uses present new and ever increasing risks that require continuing vigilance by IT security personnel and employees who use SM/W2.0 services.

PURPOSE AND GOALS:

The purpose of this policy is to provide guidance for operating units and Commerce employees to take full advantage of SM/W2.0 technologies while, at the same time, protecting Commerce and its employees by mitigating risks inherent in using these services.

This policy conforms to and implements the following:

- Guidelines for Secure Use of Social Media by Federal Departments and Agencies that were adopted by the Chief Information Officers (CIO) Council and issued in September 2009.

- President's Memorandum on Transparency and Open Government, calling for openness in Government and the establishment of a system of transparency, public participation, and collaboration, January 21, 2009.

- Office of Management and Budget (OMB) Memorandum M-10-23, Guidance for Agency Use of Third-Party Websites and Applications, June 25, 2010.

- National Archives and Records Administration (NARA) Bulletin 2011-02, Guidance on Managing Records in Web 2.0/Social Media Platforms, October 20, 2010.

- OMB's Digital Government Strategy, May 2013

- United States Office of Government Ethics' LA-15-03: The Standards of Conduct as Applied to Personal Social Media Use, April 2015

General Guidelines for the Use of SM/W2.0 Technologies in an Official Capacity:

While the following section discusses specific requirements for Department employees and operating units, each requirement is applicable to all Department operations.

(1) Department Employees:

The following are general guidelines for Department employees assigned official responsibility for operating an official account or contributing to a SM/W2.0 Web site, whether that site is hosted internally by the Department (or an operating unit) or an external commercial, academic, nonprofit, or other government agency, on behalf of the Department or an operating unit.

Department employees using SM/W2.0 technologies in an official capacity must do so only on Department-approved accounts and may only use official e-mail or other contact information for the creation and management of those accounts. In addition to helping the Department track how many accounts it possesses, using Department-approved accounts will ensure that the Department knows who is responsible for each account it uses. In the case of services that do not require accounts for the creation of a Department presence, employees should follow the service-specific guidance available on the Commerce Web Advisory Council's Social Media Website.

In general, Department employees may only post from Department-approved accounts information that represents official agency positions (i.e., not personal opinion). However, if a posting concerns a fundamental research communication as defined by the Department's Public Communications Policy (DAO 219-1) and the posting is likely to be misinterpreted as an official Department position, Department employees must clearly state that they are providing their own personal opinions and not those of the operating unit, the Department, or the Federal Government.

Department employees should conduct themselves in a professional, courteous, and honest manner in all public communications about or related to their Government work, whether online, in person, at public meetings, or in other settings.

When posting a comment related to Department work to a public Web site, Department employees must identify themselves with their Department affiliation and/or official title.

Posted information should be accurate and factual. Although there is often a tradeoff between speed of communication and accuracy, employees speaking in an official capacity should take appropriate steps to ensure that the information that they provide is correct, and whenever feasible, to correct inaccurate information about Department work (especially on Department Web sites) that is brought to their attention.

All social media updates that are posted by Department employees, or written by Department employees for dissemination or use by an outside organization, must explicitly identify the Department as the source of the content. This requirement applies to all content authored by Federal employees and contractors of the Department. Examples of "outside organizations" may include cosponsors, stakeholder groups, media organizations, and SM/W2.0 sites. Further, when representing the Department online, Department employees must not engage in discussions of opinion about the Department's programs; focus only on facts to avoid the perception that the Department is engaging in propaganda. Cite sources when providing facts.

Department employees may not post any unauthorized personally identifiable information on an SM/W2.0 Web site. Some PII may be subject to the Privacy Act and may not be released unless consistent with the provisions of the Privacy Act. Questions concerning whether employees may release PII may be directed to the CPO or the operating unit Privacy Act Officer. The improper release of PII or other sensitive information may result in civil or criminal penalties.

Department employees may not improperly use or post materials protected by copyright, trademark, patent, trade secret, data rights, or related protections for intellectual property. Proper use may require obtaining written permission from the owner of such information. The Department's Office of the General Counsel can assist employees in obtaining these permissions when necessary. Additionally, employees should exercise diligence with respect to the Department's and their operating unit's intellectual property, in logos, slogans, trademarked names, etc. Third-party use of Departmental emblems or logos requires pre-approval in accordance with DAO 201-1, Approval and Use of Seals, Emblems, Insignia and Logos.

Department employees and operating units must not endorse commercial products or services. Department employees should not post commercial advertisements or otherwise engage in activities that might lead to a conflict of interest, appearance of endorsement, affiliation, or authorization, or otherwise lead the public to believe that your operating unit supports the views, products, services, etc. of third parties. (When considering demonstrating support for local/community efforts or organizations, please contact the Office of the General Counsel to ensure that support complies with relevant Department and ethics guidance.)

Department employees may not include surveys, polls, questionnaires, etc., on official SM/W2.0 Web sites unless the questions have received Office of Management and Budget (OMB) Paperwork Reduction Act clearance. The Paperwork Reduction Act (PRA) prohibits certain information collections by the Department without prior approval by OMB. While OMB has determined that some uses of social media are not considered information collection under the PRA, please contact the Office of the General Counsel to determine if the PRA applies to a specific use.

Department employees' use of SM/W2.0 services must not include requests to contact a member of Congress, a jurisdiction, or an official of any Government (Federal, state, or local) to favor or oppose any legislation, law, or appropriation because these activities are prohibited by the Anti-Lobbying Act.

Department employees may not solicit consensus advice from the public using SM/W2.0 technologies**.** The Federal Advisory Committee Act prohibits agencies from receiving consensus advice from *de facto* committees or groups who are not made up entirely of Federal employees.

(2) GUIDELINES FOR USE OF SM FOR OPERATING UNITS:

Department Web sites, pages, etc. that contain postings by an operating unit or the public require diligent monitoring.

Because monitoring and filtering of Department Web sites, pages, etc. may give rise to public criticism, operating units are required to use either the Office of the Secretary's comment policy or develop and post their own comment policy approved by the Office of the General Counsel. Operating units should post commenting guidelines prominently, when technically able to do so, and apprise public users of it regularly. Operating units using SM/W2.0 technologies must prevent the posting of or immediately delete postings by the public that contain:

- Comments regarding a political party or a candidate in a partisan political campaign (a campaign in which candidates are identified by political party);

- Requests to contact a Member of Congress or official of any government, to favor or oppose any legislation, law, or appropriation;

- Advertisements, endorsements, or promotions; and

- Vulgar or abusive language, personal attacks of any kind, or offensive terms targeting individuals or groups.

All social media updates that are posted by operating units, or written by operating units for dissemination or use by an outside organization, must explicitly identify the Department as the source of the content. This requirement applies to all content authored by Federal employees and contractors of the Department. Examples of "outside organizations" may include cosponsors, stakeholder groups, media organizations, and SM/W2.0 sites. Further, when representing the Department online, operating units must not engage in discussions of opinion about the Department's programs; focus only on facts to avoid the perception that the Department is engaging in propaganda. Cite sources when providing facts.

Operating units must ensure that the content maintained on their SM/W2.0 sponsors' Web sites, especially PII and other sensitive information, is secure and adequately safeguarded from unauthorized disclosure or destruction. The records must be retained consistent with the Department's records retention requirements. NARA Bulletin 2011-02, Guidance on Managing Records in Web 2.0/Social Media Platforms, provides additional guidance.

Operating units interacting with the public through SM/W2.0 technologies must ensure that such interactions require and generate the least amount of PII possible from their users. To that end, and whenever feasible, operating units must edit and actively manage their SM/W2.0 Web site or application

settings to make sure that only the minimum amount of PII necessary to effectively use such technologies is being generated/collected. OMB Memorandum M-10-23 establishes requirements for a PIA, which must document the agency's decision process. Agencies should discuss these details as appropriate in the privacy notice posted to the SM/W2.0 technology, as described in OMB Memorandum M-10-23.

Department Web sites must not collect any personal information from children (under the age of 13) in violation of the Children's Online Privacy Protection Act.

When posting information using SM/W2.0 technologies, operating units should ensure and maximize the quality, objectivity, utility, and integrity of posted information (including statistical information), and ensure that measures are in place to allow for the correction of information not meeting that standard. This is required under the Department's Information Quality Act Guidelines.

Operating units are required to ensure that people with disabilities or limited English proficiency have an accessible version of official content posted online, in compliance with Section 508 of the Rehabilitation Act of 1973, and Executive Order 13166, Improving Access to Services for Persons With Limited English Proficiency. Materials posted to SM/W2.0 services also must be posted in accessible formats on the official Department Web site; non-governmental SM/W2.0 sites may not be the sole location where content is posted. This will ensure that people with disabilities, or who have limited English proficiency, always have an accessible version of the content and that the official version of the content is located on a Department Web site.

If the SM/W2.0 technology allows the public to respond to official postings, the Department Web site also must provide visitors with the ability to communicate with the Department so that members of the public do not have to register with or provide personal information to third-party Web sites that may require registration or the provision of personal information. The Department Web site must provide an alternative way, e.g., e-mail address for members to communicate directly with the Department without providing personal information to a third-party Web site.

When visitors to an official Department Web site are redirected from the Department site to a third-party site, the visitors must be notified that they are leaving the official agency site, e.g., when a visitor to a Commerce site is redirected to view a video on YouTube®. The Department's notification should include an exit disclaimer stating that (1) the Department cannot attest to the accuracy of the information provided by a non-Federal

Government site; (2) the link to the site is provided only for reference; and (3) the link to the site does not constitute endorsement of any product, service, organization, company, information provider, or content. Further, Department employees' use of links to such third-party sites must be consistent with their operating unit's linking policy. This is required by OMB Memorandum M-05-04, Policies for Federal Agency Public Web Sites, and OMB Memorandum M-10-23, Guidance for Agency Use of Third-Party Websites and Applications, June 25, 2010.

The Department may not rely on SM/Web 2.0 technologies as the exclusive means of distribution of information. Original materials posted to SM/W2.0 services also must be posted on official Government Web sites, *and* alternative, non-electronic forms of information must be made available upon request, pursuant to OMB Circular A-130, Management of Federal Information Resources.

(3) Hatch Act in the Workplace:

Department employees are prohibited by the Hatch Act from engaging in political activity on Government premises or using Government resources. Political activity includes any activity directed toward the success or failure of a political party or a candidate in a partisan political campaign. Thus, official use of social media may not include any reference relating to a political party, candidate, or campaign, including links to political websites or organizations.

Additional information is available from the OGC Ethics Law and Programs Division Web site, by phone at 202-482-5384, or via e-mail at ethicsdivision@doc.gov.

Applying for Official SM/W2.0 Accounts

Commerce employees should consult the list of Commerce approved Social Media and Web 2.0 Web sites and use the Web-based Commerce Social Media Application process (registration required) to apply for SM/W2.0 accounts. The process is overseen by the Office of the Secretary's Office of Digital Engagement, with input from operating unit's public affairs and chief information offices. The Office of General Counsel will be consulted as necessary.

General Guidelines for the Use of SM/W2.0 Technologies in an Unofficial Capacity:

The following are general guidelines for Department employees' unofficial or personal use of SM/W2.0 technologies. Please note that these guidelines for unofficial or personal use do not apply to Department contract employees, except to the extent that they are using Department resources to provide information to the public.

(1) Personal and Professional Communication:

Pursuant to the Department's Public Communications Policy (DAO 219-1), Department employees on Government or non-Government Web sites, who wish to post or upload original material that is not publicly available using SM/W2.0 technologies that relates to the programs or operations of their operating unit and that is related to their official duties, must submit their communication for review to their supervisor or a public affairs officer or other appropriate communications staff at their operating unit. A personal account must never be the first point of release for public documents.

Employees should be mindful of blurring their personal and professional life when using SM/W2.0 technologies. Employees should not establish relationships with working groups or affiliations that may reveal sensitive information about their job responsibilities.

Pursuant to section 7 of DAO 219-1 (Public Communications), researchers are free to participate in Fundamental Research Communications with the media and members of the public regarding their research in their unofficial capacity on personal social media accounts, but they are not required to do so. Given the nature of the scientific process, the role of the scientific community is to draw scientific conclusions based on available data. Department researchers may draw scientific conclusions based on research related to their jobs and communicate those conclusions to the public and the media in a Fundamental Research Communication. However, if such a conclusion could reasonably be construed as representing the view of the Department or an operating unit when it does not, then the researcher must make clear that he or she is presenting his or her individual conclusion and not the views of the Department or an operating unit.

Although Department employees are encouraged to learn about and experiment with these tools in an unofficial capacity, they should be mindful that any information posted on the Web, even when on-site privacy controls are used on SM/W2.0 sites, could become public.

Do not disclose any information obtained on the job that is not already publicly available. This includes national security (classified) information, personally identifiable information, proprietary or business confidential information, pre-decisional information, or similar sensitive information.

The Commerce Internet Use Policy allows employees to use their Government computer and SM/W2.0 for their personal use, provided that access is permitted by the operating unit CIO and use of equipment is minimal. Additionally, use of SM/W2.0 must not interfere with office operations or involve commercial activities (profit-making or business), partisan political activities, or sexually explicit communications.

(2) Employee Title Use:

You may use your title when it is self-evident that you are not posting in an official capacity, such as posting a resume or listing your employment history on a social network profile.

Use of your job title in social media profiles must be considered within the totality of the circumstances to determine whether a reasonable person with knowledge of the relevant facts would conclude that the government sanctions or endorses your communication.

Relevant factors to consider in making the determination include:

- Whether you state that you are acting on behalf of the government;
- Whether you refer to your connection to the government as support for your statements;
- Whether you prominently feature your agency's name, seal, uniform or similar items on the social media account or in connection with specific social media activities;
- Whether you reference government employment, title, or position in areas other than those designated for biographical information;
- Whether you hold a highly visible position in the Government, such as a senior or political position, or are authorized to speak for the Government as part of your official duties;
- Whether other circumstances would lead a reasonable person to conclude that the government sanctions or endorses your social media activities; or
- Whether other circumstances would lead a reasonable person to conclude that the government does not sanction or endorse your social media activities.

Ordinarily, an employee is not required to post a disclaimer disavowing government sanction or endorsement on the employee's personal social media account. Where confusion or doubt is likely to arise regarding the personal nature of social media activities, you are encouraged to include a disclaimer clarifying that your social media communications reflect only your personal views and do not necessarily represent the views of your agency or the United States. A clear and conspicuous disclaimer will usually be sufficient to dispel any confusion that arises.

(3) HATCH ACT ON PERSONAL ACCOUNTS:

The Hatch Act prohibits Federal employees from soliciting, accepting, or receiving campaign contributions, including through the use of SM/W2.0 technologies. This prohibition includes hosting or posting to a Web site that includes a link for making contributions to a political party or a candidate in a partisan election, that is, a campaign in which candidates are identified by political party.

Further, Department employees are prohibited by the Hatch Act from engaging in political activity on Government premises or using Government resources. This restriction includes using personal or Government devices for such purposes. Political activity includes any activity directed toward the success or failure of a political party or a candidate in a partisan political campaign.

Additional information is available from the OGC Ethics Law and Programs Division Web site, by phone at 202-482-5384, or via e-mail at ethicsdivision@doc.gov.

OTHER APPLICABLE COMMERCE POLICIES

The use of SM/W2.0 services must conform to other applicable Commerce policies, including the following:

- Department's Public Communications Policy (DAO 219-1) , provides guidance for employees for communicating with the public about Commerce programs and activities and describes the role of the Office of Public Affairs (OPA) in ensuring that public communications are open and accurate, April 30, 2008.

- Web Policies and Best Practices developed by the Commerce Web Advisory Council and adopted by the Commerce CIO and Director of Public Affairs for implementation Commerce-wide, provide general guidance and requirements for the display of content on the Web.

- Commerce Internet Use Policy, provides general guidance regarding Internet use by Department of Commerce personnel (employees, contractors, associates, and others) who are authorized to use Commerce resources, December 19, 2008.

RESPONSIBILITIES OF CHIEF INFORMATION OFFICERS

RISK ASSESSMENT AND AUTHORIZATION FOR USE:

Before any SM/W2.0 service or technology is approved for use on any Commerce network or system, the responsible operating unit Chief Information Officer (CIO) must assess whether the users in the operating unit should be authorized to use or access a particular SM/W2.0 technology using established risk management methodologies. The relevant CIO should determine whether any risk-based limitations on access or usage by users within that operating unit are warranted prior to authorizing the use of a particular service or technology. The risk assessment should be conducted in accordance with the risk management principles in NIST Special Publication 800-30 (as amended), Guide for Conducting Risk Assessments, and other NIST Publications that apply. Additional guidance for CIOs is in the Guidelines for Secure Use of Social Media by Federal Departments and Agencies.

A CIO's authorization to use a particular SM/W2.0 service or technology applies only to the operating unit for which the CIO is responsible. Depending on the level of IT security measures in place, a CIO may approve use of or access to a SM/W2.0 service on particular operating unit networks or systems but not others. Each CIO is responsible for maintaining a current inventory of SM/W2.0 technologies approved for access from their operating unit network(s) and systems.

TERMS OF SERVICE AND PRIVACY:

After assessing the risks, the relevant CIO must verify that the SM/W2.0 service provider terms of service agreement has been approved by the Department of Commerce, including the Department's Office of the General Counsel, before authorizing Commerce employee use of that service or technology. Approved service agreements are on the Commerce Web Advisory Council Social Media Web site.

OMB M-10-23 requires agencies to conduct a Privacy Impact Assessment (PIA) in all situations in which any personally identifiable information (PII) will become available to the agency. OMB M-10-23 also requires agencies to update agency privacy policies and post specialized privacy notices on the actual SM/Web 2.0 service itself, to the extent possible. Each responsible

operating unit CIO must coordinate these activities with the Departmental Senior Agency Official for Privacy.

The Commerce CIO is responsible for oversight and monitoring of implementation of this policy by operating unit CIOs.

SPECIFIC IT SECURITY GUIDELINES FOR USING SM/W2.0 TECHNOLOGIES

SM/W2.0 present IT security challenges beyond those of static Web sites, and it is essential to adhere to applicable Federal and Department IT security requirements, including the following:

- The Administrative Point of Contact (APOC) for a SM/W2.0 account is the individual who is solely responsible and accountable for the administration, password control, and access management of the account. An APOC may be anyone approved by the operating unit's Office of Public Affairs, Office of the Chief Information Officer and the Office of Digital Engagement through the Social Media Application process.

- APOCs should not use the same password for more than one account. Many SM/W2.0 sites allow account administrators to assign administrative rights to other users. When available, this feature should be used.

- APOCs must not use the same password for logging in to their Commerce or operating unit network that they use to access any SM/W2.0 site. Failure to use different passwords could compromise the security of the Commerce or operating unit network.

- APOCs should use two-factor authentication for all accounts where it is available and possible.

- Even in cases where SM/W2.0 Web sites do not enforce strong password requirements, strong passwords should be used in accordance with CITR-009: Password Requirements for password length, expiration, and complexity, e.g., use of upper and lower case letters and special characters.

- APOCs should assess and accept risk for accounts prior to putting content on a service and work with IT security community to

complete a full risk assessment at the enterprise level. This is separate from accepting the Terms of Service.

- APOCs document areas where policy cannot be followed, e.g. using a government account to manage Facebook sites when Facebook does not allow individuals to have more than one account at a time.

- APOCs should only follow links and download files from known and secure sources. Any file downloaded from a SM/W2.0 site must be virus scanned before opening. Upon receipt of a suspicious message, link, or file to download from a known person, APOCs should verify that the item was actually sent by the person before virus scanning and opening it.

- SM/W2.0 accounts must be monitored on a regular basis. In the event pages are hacked or defaced, a report must be sent immediately to DoC Computer Incident Response Team (CIRT) or the operating unit's IT Security Officer. After reporting the incident, the APOC for the account must contact the software or service provider to regain control of the account and restore the page. Passwords will be changed immediately after any hack or page defacement.

RESOURCES FOR ADDITIONAL INFORMATION

• Office of the General Counsel, General Law Division, 202-482-5391.

• Office of the General Counsel, Ethics Law and Programs Division, 202-482-5384 or ethicsdivision@doc.gov).

• Office of the General Counsel, Employment and Labor Law Division, 202-482-5017

• Office of IT Policy and Planning, OCIO, 202-482-0275.

• Director of Digital Engagement, OSEC OPA, 202-482-2556

• Chief Privacy Officer and Director of Open Government, 202-482-3463

• Records Management Officer, OCIO, 202-482-4559